POLICY INFORMATION

Document # **200**	Title: **Security Management Process**	Print Date: **9/06/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Administrative**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B867 10B5491...	Date Approved: 9/19/2016

I. POLICY STATEMENT

CEHS will take reasonable and appropriate precautions to prevent, detect, contain, and correct security violations.

II. DEFINITIONS

See HIPAA Privacy Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Component/HCC (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

1. **System Identification and Tracking -** The person responsible for HIPAA compliance within each HCC is responsible for identifying and maintaining an inventory of the information system(s) managed within that component. When a new information system is implemented, that responsible person will follow applicable USU policy regarding approval, purchasing and implementation of new information systems.
2. **Risk Assessment Program -** The CEHS Privacy and Security Officer(s) will establish a program to identify and mitigate risks to PHI.

   Risk Analysis - Each HCC shall complete a risk analysis:

   i. Annually;
   ii. Whenever a new information system is implemented;
   iii. In response to newly-recognized risk(s) that have identified as a result of activity reviews, security incidents, or environmental or operational changes.

3. **Completing the Risk Assessment:** Risk Assessments can involve some or all of the following individuals:

- HCC Privacy Officer

- HCC Director
- HCC Department Head
- CEHS Security and Privacy Officer(s)
- USU Information Security Office

Step One: Each HCC will identify and document where confidential or sensitive data, including PHI, is created, received, maintained, processed or transmitted. Both physical boundaries as well as logical boundaries covering the media containing the confidential or sensitive electronic data, including PHI, regardless of its location should be documented. Each HCC shall also take into consideration any remote workforce removable media and portable computing devices (e.g. laptops, removable media and backup media).

Step Two: The HCC will gather all information requested by the Security and Privacy Officer(s) as well as identify (1) the conditions under which the confidential or sensitive electronic data, including PHI, is created, received, maintained, processed or transmitted by the HCC; and (2) the security controls currently being used to protect the data. An assessment of current security controls shall be performed.

Step Three: Using the Physical Safeguards Assessment form and the Data Safeguards Assessment form that are attached to this document, the HCC will identify potential threat sources and vulnerabilities that are applicable to the HCC and could have a negative impact on the HCC's ability to protect PHI. A report listing each threat should be compiled. Some examples of common threat sources are listed in the table below:

Type	Examples
Natural	Flood, earthquake, tornado, landslide, storms, etc.
Human	Unintentional human acts such as inadvertent data entry or deliberate acts such as unauthorized access to confidential information.
Environmental	Long-term power failure, pollution, chemicals, etc.

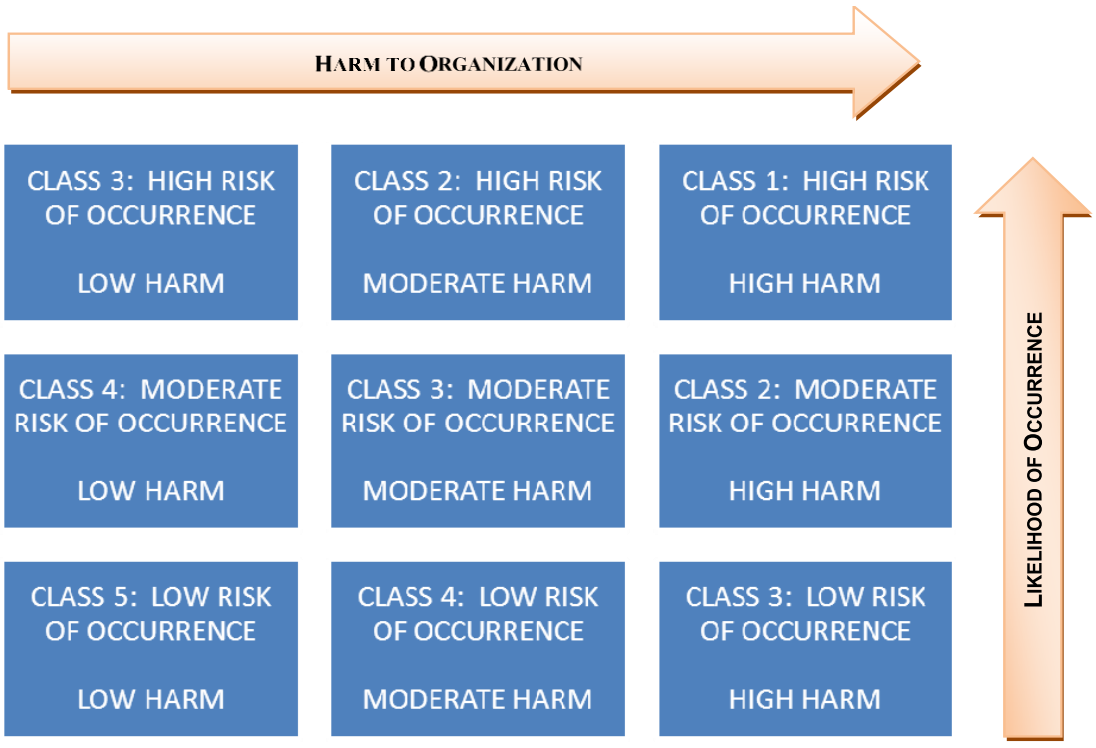
Step Four: Determine the likelihood and impact of each threat. The system and data sensitivity can be determined based on the level of protection required to maintain the confidential data, including PHI's confidentiality, integrity and availability. The adverse impact of a security event can be described in terms of the loss of any, or a combination of any, of the following three security objectives; integrity, availability and confidentiality. The table below provides a brief description of each security objective and the impact of its not being met.

Security Objective	Impact Description
Loss of Confidentiality	System and data confidentiality refers to the protection of information from unauthorized disclosure. Unauthorized, unanticipated or unintentional

	disclosure could result in loss of public confidence, embarrassment, or legal action against the HCC and CEHS.
Loss of Integrity	System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all of these reasons, loss of integrity reduces the assurance of an IT system.
Loss of Availability	If a mission-critical IT system is unavailable to its end users, CEHS's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Step Five: Determine the risk level by taking into account the information acquired in all of the previous steps. The level of risk should be determined by analyzing the values assigned to the likelihood that a threat could occur, and the impact of the threat occurrence.

The following Risk Management Model can provide help in classifying the level of risk and potential harm to the organization:



Once classified, the following response and timeframes should be used:

CLASS	RISK	RECOMMENDED ACTION
Class 1	High Risk, High Harm	Allocation of resources necessary to accept, avoid, transfer or mitigate the risk within 48 hours.
Class 2	High Risk, Moderate Harm Moderate Risk, High Harm	Allocation of resources necessary to accept, avoid, transfer or mitigate the risk within 30 days.
Class 3	Moderate Risk, Moderate Harm Low Risk, High Harm High Risk, Low Harm	Allocation of resources necessary to accept, avoid, transfer or mitigate the risk within 60 days.
Class 4	Low Risk, Moderate Harm Moderate Risk, Low Harm	Review of the risk in order to determine the appropriate action. Such action may include allocation of resources to accept, avoid, transfer or mitigate the risk. Assumption of this risk should not be considered an option.

Risk Mitigation and Monitoring: The CEHS Security Officer will recommend and monitor the effectiveness of security measures designed to reduce risks and vulnerabilities to a reasonable and appropriate level. More specifically these measures are designed to reasonably and appropriately:

- Protect the Confidentiality, Integrity, and Availability (CIA) of all PHI that CEHS HCC creates, receives, maintains or transmits.
- Protect against any reasonably anticipated threats or hazards to the CIA of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule.
- Facilitate workforce compliance.

4. **Information System Activity Reviews -** The Security Officer and applicable system administrator will:
    a. Regularly perform Information System Activity Reviews (e.g., audit logs and trails, information system activity records, facility access records) for the purpose of detecting:
        i. Unauthorized access to PHI:
        ii. Unusual patterns of use or activity; and
        iii. Other potential security violations.
    b. Document the findings of the System Activity Review. Documentation shall be retained for at least six years from the date of review; and
    c. Report suspicious finding in accordance with the security incident reporting mechanisms established by CEHS.

5. **Security Incident Detection, Response and Reporting -**
   CEHS Privacy and Security Officer(s) will develop, document, and implement procedures to:
   a. Identify possible security incidents;
   b. Respond to suspected or known security incidents;
   c. Mitigate, to the extent practical, harmful effects of known security incidents; and
   d. Document and report security incidents and their outcomes. All documentation relating to potential and verified security incidents will be retained for at least six years from the date of documentation.
6. **Risk Acceptance -** There could be situations where a risk is reviewed and a determination is made that the risk is acceptable for the HCC's environment. When accepting the risk results in (1) an information system, a communications system, or an organizational unit being out of compliance with CEHS policies and procedures and/or standards, and (2) the responsible HCC Director does not intend to come into full compliance within the timeframe prescribed by CEHS policy, the Risk Acceptance form must be prepared and submitted to the CEHS Privacy/Security Officer(s).
7. **Risk Avoidance -** The risk is reviewed and a determination is made that the risk can be removed from the HCC environment by removing the source of the risk. This could include removal of the application, host, platform or other system that contains the identified risk.
8. **Risk Transfer -** The risk is reviewed and a determination is made that the system capability is required but can be transferred to a third party vendor or provider. Although such a transfer is an acceptable method for managing risk, it does not relieve the facility of compliance with a security policy or procedure.

V. ATTACHMENTS

Attachment A - Physical Safeguards Assessment Form

Attachment B - Data Safeguards Assessment Form

Attachment C - Risk Acceptance Form

VI. REFERENCES

45 CFR §164.308 (a)(1)

Attachment A

Physical Safeguards Assessment Form

DEVICE AND MEDIA CONTROLS
To meet these requirements, an organization must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain confidential or sensitive electronic information, including electronic protected health information into and out of the premises, and the movement of these items within the premises.

1. Does the department utilize policies and procedures that govern the receipt and removal of hardware and electronic media that contain confidential or sensitive electronic information, including ePHI into and out of the premises?
□ Yes
□ No
□ Don't know
□ This is managed by _____

2. Does the department utilize policies and procedures that govern the movement of hardware and electronic media that contain confidential or sensitive electronic information, including ePHI within the premises?
□ Yes
□ No
□ Don't know
□ This is managed by _____

3. Does the department utilize implemented policies and procedures to address the FINAL disposition of confidential or sensitive electronic information, including ePHI, and/or the hardware or electronic media on which it is stored?
□ Yes
□ No
□ Don't know
□ This is managed by _____

4. Does the department utilize policies and procedures for removal of confidential or sensitive electronic information, including ePHI from electronic media before the media is made available for re-use?
□ Yes
□ No
□ Don't know
□ This is managed by _____

5. Does the department utilize policies and procedures for maintaining a record of the movements of hardware and
electronic media and any person responsible for these movements?
□ Yes
□ No
□ Don't know
□ This is managed by _____

6. Does the department utilize policies and procedures for the creation of a retrievable, exact copy of confidential or sensitive electronic information, including electronic protected health information, when needed, before movement of equipment?
□ Yes
□ No
□ Don't know
□ This is managed by _____

7. If yes, are these policies and procedures practiced consistently in the department?
□ Yes
□ No
□ Don't know

NOTES: (Attach copy of policy and/or add notes here)
_____

_____

_____

_____

ADDITIONAL ASSESSMENT QUESTIONS:

1. Does the department possess fire suppression systems (Class C extinguishers or sprinklers)?
□ Yes
□ No
□ Don't know

2. Does the site have working modems attached to any of the desktop workstations?
□ Yes
□ No
□ Don't know

3. Are there any ancillary or free standing computer systems at this site? (Not attached to the network?)
□ Yes
□ No
□ Don't know

4. Are there any wireless access points or wireless workstations within or managed from this department?
□ Yes
□ No
□ Don't know

5. Are there any closets or rooms that contain networking or switching equipment?

□ Yes
□ No
□ Don't know

6. Are there any network connections that are not in use in the department?
□ Yes
□ No
□ Don't know

7. a. Are there any fax machines in the department?
□ Yes
□ No
□ Don't know
b. If yes, are these fax machines accessing confidential or sensitive electronic information, including ePHI (such as imaging or faxback service) or are they plain paper faxes?
□ Plain paper faxes only
□ Faxback systems
□ Imaging systems
□ Access other electronic PHI

8. Is the staff aware and have they been trained in the need for security of confidential or sensitive electronic information, including ePHI?
□ Yes
□ No
□ Don't know

Assessment Performed by (Print): _____

Date: _____ Signature: _____

Job Title: _____

Attachment B

Data Safeguards Assessment Form

WHEN TO USE THIS FORM: This form should be used on a Clinical or departmental basis to identify any physical security risks and vulnerabilities that exist in a HCC. This form should be used when the area inspected contains confidential or sensitive electronic information, including electronic Protected Health Information (ePHI). This form should be used in the risk assessment to identify security risks and vulnerabilities that exist in the HCC.

Data Center Name: Date:

Facility Name:

Facility Location:

Inspection Performed by:

Fire Damage Exposure In reference to local facility fire protection related environment of care standards:	**Y/N**	**Rectify/Improve (H/M/L)**
1. Is the data center housed in a building that meets local facility fire protection related environment of care standards?		
2. Are the areas surrounding the data center protected from fire?		
3. Are the raised floor tiles and/or hung ceiling tiles non-combustible?		
4. Can the walls, doors, partitions, floors, furniture and window coverings in the data center meet local facility fire protection related environment of care standards for resisting the spread of fire?		
5. Does the data center have automatic fire extinguishing systems?		
6. Are flammable and otherwise dangerous materials and activities prohibited from the data center and surrounding areas?		
7. Are paper and other supplies stored outside the computer/network operations area		
8. Is there fire and smoke detection equipment in the data center?		
9. Are portable fire extinguishers available?		
10. Are clear and adequate fire instructions clearly posted?		
11. Is the fire department telephone number clearly posted?		
12. Are fire alarm switches clearly visible, unobstructed and easily accessible at points of exit?		
13. Can the fire alarm be activated manually?		
14. Does the alarm sound:		

• Outside of the data center? • At the receptionist's area?		
15. Is there an emergency evacuation exit, different than the main exit?		
16. Is there an evacuation plan posted?		
17. Does emergency power shut down the air conditioning?		
18. Are fire and smoke detection equipment checked and tested per requirements?		
19. Can emergency crews easily gain access to the data center?		
20. Are fire drills held per requirements?		

Water Damage Exposure	**Y/N**	**Rectify/Improve (H/M/L)**
1. Is the network and computing equipment above ground and protected from flooring?		
2. Is there a drainage system in the area of the data center?		
3. Can the data center ceiling protect the room from leaks in overhead water pipes?		
4. Are floor-level electrical junction boxes protected?		
5. Are there moisture sensors at the lowest points of the data center?		

Other Natural Disaster Exposures	**Y/N**	**Rectify/Improve (H/M/L)**
1. Can the building housing the data center withstand: • High winds? • Tornadoes? • Earthquakes?		
2. Is the data center and equipment grounded for protection against lightning?		

Electricity and Telecommunications	**Y/N**	**Rectify/Improve (H/M/L)**
1. Are generators and transformers located outside of the data center?		
2. Is there an emergency lighting system in the data center?		
3. Is the fresh air intake located above ground level and away from smoke stacks and sources of combustible dust and gas?		
4. Are air conditioning and emergency shut-off switches linked?		
5. Are switches easily accessible?		

Climate Control	**Y/N**	**Rectify/Improve (H/M/L)**
1. Is the air conditioning system and power supply for the data		

center separate from the rest of the building?		
2. Is there backup air conditioning available?		
3. Is the fresh air intake located above ground level and away from smoke stacks and sources of combustible dust and gas?		
4. Are air conditioning and emergency shut-off switches linked?		

Facility Access Control	**Y/N**	**Rectify/Improve (H/M/L)**
1. Are there procedures to guard against vandalism, sabotage, and unauthorized intrusion?		
2. Are there windows that can be broken to gain access to the data center?		
3. Are there procedures for data center personnel to handle: • Unauthorized intruders? • Bomb threats? • Notifying the local police?		
4. Are security devices checked and tested on a regular basis?		
5. Do any of the following pose a threat to the data center based on their proximity to the data center: • Loading ramps? • Cafeteria or workshops? • Storage areas? • Outside walls? • Power panels? • Heavy usage of electrical equipment?		
6. Are there access controls during regular and off-hours? • To other departments? • To the computer room? • To the network room?		

General Housekeeping	**Y/N**	**Rectify/Improve (H/M/L)**
1. Is the data center kept clean and orderly?		
2. Are food and beverages prohibited in the data center or at least confined to a designated area?		
3. Is smoking banned in the data center?		
4. Is there a media cleaning and rotation schedule?		

Organization and Personnel	**Y/N**	**Rectify/Improve (H/M/L)**
1. Are there company personnel responsible for data center		

security?		
2. Does management have procedures for handling disgruntled employees?		
3. Have recovery teams been selected in case of a disaster?		
4. Are there disaster plans in place?		

Backup and Recovery	**Y/N**	**Rectify/Improve (H/M/L)**
1. Is there an inventory of critical applications and data?		
2. Have specified task assignments been made for all personnel for recovery strategy procedures?		
3. Are duplicate data files and copies of all computer programs stored at another location?		
4. Are backup computer systems available? If so, can they adequately handle critical processing requirements of failed unit(s)?		

Device and Media Controls	**Y/N**	**Rectify/Improve (H/M/L)**
1. Is there an inventory list of media such as tapes and disks?		
2. Do procedures exist for controlling media storage?		
3. Is the alternate storage site protected from fire, flood, dust, vandalism, theft, etc.?		
4. Is access to the media storage area restricted to authorized personnel only?		

Operational Procedures	**Y/N**	**Rectify/Improve (H/M/L)**
1. Are procedures in place outlining procedures for operation of network and computing equipment?		
2. Is operational staff aware and trained in these procedures?		
3. Are contact names for vendors, maintenance providers, contractors, utility and telecom providers and facilities management for both normal and non-business hours maintained in a place known by operations staff?		
4. Does operations staff have pagers or a call out list to be used in case of an emergency?		
5. Is there a contact list for contacting senior management during non-working hours?		

Client/Server Equipment Risks	**Y/N**	**Rectify/Improve (H/M/L)**

1. Are all server hardware, software configurations and revision levels documented?		
2. Are all client workstations hardware and software configurations and revision levels documented?		
3. Are identified hardware spares available if needed for critical servers?		
4. Are all network equipment hardware and software configurations and revisions documented?		
5. Is critical operating system, applications, and network software stored off site?		
6. Do alternate processing sites exist?		

Internet/Intranet Systems/Network Risks Do current resources:	**Y/N**	**Rectify/Improve (H/M/L)**
1. Know how to detect and recover from sophisticated and automated firewall and system probing?		
2. Know how to detect and recover from NFS attacks?		
3. Know how to detect and recover from e-mail attacks?		
4. Know how to detect and recover from compromised vendor default user names and passwords?		
5. Know how to detect and recover from spoofing/sniffing/fragmentation and splicing attacks?		
6. Know how to detect and recover from social engineering attacks?		
7. Know how to detect and recover from prefix scanning (scanning of company phone numbers to detect MODEM lines and thereby bypassing some security checks)?		
8. Know how to detect and recover from denial of service attacks (system floods)?		
9. Know how to detect and recover from systems/network scanning and probing attacks?		
10. Know how to detect and recover from password theft?		
11. Know how to detect and recover from privilege grabbing (exploiting start-up files) attacks?		
12. Know how to detect and recover from hostile code (viruses, Trojan horses, backdoors for repeated hacking) attacks?		
13. Know how to detect and recover from e-vandalism (web page defacing or loss) attacks?		
14. Know how to detect and recover from data theft?		
15. Know how to detect and recover from spamming?		

16. Know how to detect and recover from e-terrorism?		
17. Know how to detect and recover from system infrastructure attacks?		
18. Know how to detect and recover from logic time bombs effecting backup tapes?		
19. Know how to detect and recover from stealth viruses?		
20. Know how to detect and recover from laptop theft?		

Assessment Performed by (Print Name):_____

Date: _____Signature: _____

Job Title: _____

Attachment C

Risk Acceptance Form

WHEN TO USE THIS FORM: This form must be employed when (1) an information system, a communications system, or an organizational unit is known to be out of compliance with CEHS information security policies and/or standards, and (2) the responsible manager does not intend to come into full compliance within the timeframe prescribed by CEHS policy.

RISK ACCEPTANCE

Regarding policy or procedure number _____, dealing with the topic of:
_____.

I understand that compliance with CEHS Security Policies and Procedures is expected for all departments, organizational units, and information and communication systems. I have read the above-named policy or procedure and I believe that the control(s) described therein should not be required for the following department, organizational unit, and information or communication system.

I furthermore understand that a control deficiency in one information system can jeopardize other information systems because erroneous data may be inherited, or because a conduit for an intruder to enter CEHS systems may be created. I also understand that non-compliance in this instance may adversely affect the morale or willingness of staff associated with other systems to comply with information security policies and standards. I understand that an exception to Information Security Policies and Standards is appropriate only when it would: (a) adversely affect the accomplishment of CEHS business, and/or (b) cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance. I believe that an exception to this policy or standard is warranted because:

_____

_____

_____

I have prepared, or have had a staff member reporting to me prepare, a written assessment of the risks associated with being out of compliance with the above-mentioned policy or procedure. This risk assessment has been reviewed and approved by the designated system owner and the HCC system administrator. I accept responsibility for this decision to be out of compliance with Policies and/or Procedures. Responsibility means that my job performance evaluation, my salary and bonus, and my continued employment status at CEHS can be jeopardized or damaged if a major loss takes place because this out of compliance situation existed. I also understand that this exception will expire one year from the date the above-mentioned approvals are obtained.

_____ _____

Signature of responsible manager Date signed

_____

Printed name of responsible manager

Procedural Note: If this out of compliance situation is to continue, the brief risk assessment regarding the out of compliance situation must be updated annually, the above-mentioned approvals must be obtained annually, and this form must be signed by the responsible manager annually. Each year the responsible manager must return a signed copy of this form to the Privacy and/or Security Official(s).